UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 151 South 9th Street, Unit F, La Puente, California	)	Case No. 8:18-MJ-00673

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 922(m), 922(b)(2), 924(a)(3)(A), 923(g)(1)(A), and 922 (a)(1)(A)	Licensed dealer making false entry in a required record, selling or delivering any prohibited firearm in violation of state law, making any false statement in required records, and failing to maintain records; and dealing in firearms without a license

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of_____days (*give exact ending date if more than 30 days*:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jacob Boyd, United States Postal Inspector

Printed name and title

Sworn to before me and signed in my presence.

Date: _____

Judge's signature

City and state: Santa Ana, CA

Honorable Douglas F. McCormick

Printed name and title

AUSA: Daniel Ahn x3539

AFFIDAVIT

I, Ludger A. Parent, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") and have been so employed since August 2000. I completed the Criminal Investigations Training Program at the Federal Law Enforcement Training Center in Brunswick, Georgia. I also completed the ATF Special Agent Basic Training at the National Training Academy in Brunswick, Georgia. During those courses of study, I received training in the investigation of federal firearms and narcotics violations. Before becoming an ATF SA, I was employed as an Inspector with the U.S. Customs Service for approximately five years.

2. I have conducted numerous investigations involving the possession and use of firearms and narcotics. While employed as an ATF agent, I have been involved in investigations dealing with the possession, manufacture, distribution, and importation of firearms, as well as controlled substances. I have also participated in the undercover purchase of firearms and narcotics.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of a search warrant for the premises known as EXA Tactical Firearms, located at 151 South 9th Street, Unit F, La Puente, California (the "**SUBJECT PREMISES**"). EXA Tactical Firearms is a federal firearms

licensee ("FFL"). Based on the facts set forth below, there is probable cause to believe that Mr. and Mrs. Pet, LLC, DBA "EXA Tactical Firearms" ("EXA Tactical Firearms") and specifically the owner and licensee, Devin Wenhua Lee ("LEE") is in violation of Title 18, United States Code, Section 922(m) (Licensed Dealer Knowingly Making Any False Entry In A Required Record); Section 922(b)(2) (Licensed Dealer To Sell Or Deliver Any Prohibited Firearm To A Person In Violation Of State Law); Section 924(a)(3)(A) (Licensed Dealer Makes Any False Statement Or Representation Kept In Required Records); Section 923(g)(1)(A) (Licensed Dealer Failure To Maintain Records); and Section 922(a)(1)(A) (Dealing Firearms Without A License).

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. SUMMARY OF PROBABLE CAUSE

5. In July of 2018, two former employees of EXA Tactical Firearms contacted ATF regarding owner LEE. They stated that on several occasions LEE falsified the required state and federal firearm transaction records in order to sell "unsafe" (law enforcement only) handguns, which are in high demand on the

secondary market, to otherwise prohibited persons. ATF inspections of EXA Tactical Firearms (i.e., the **SUBJECT PREMISES**) in 2014 and 2015 revealed numerous violations, including the failure to completely record firearm acquisitions and dispositions in the Acquisition and Disposition ("A&D") record, and failure to report multiple sales. A review of available records from ATF and California firearms registration databases, as detailed below, reveal that EXA Tactical Firearms and LEE at the **SUBJECT PREMISES** have continued, through at least October 2018, to improperly record firearm acquisitions and dispositions in order to sell firearms to individuals in the State of California who would otherwise be prohibited persons.

PREMISES TO BE SEARCHED

6. The **SUBJECT PREMISES** is described as follows, and is more fully described in Attachment A:

a. The premises known as 151 South 9th Street, Unit F, La Puente, California, including all rooms, attics, storage rooms, garages or all outbuildings of any kind, attached or unattached, including all safes located on the premises. Unit F is located on the top floor of a tan stucco two story structure. The front door faces west at the north end of the structure and the letter "F" appears on the door.

ITEMS TO BE SEIZED

7. The items to be seized from the **SUBJECT PREMISES** are described as follows, as more fully described in Attachment B:

a. Any and all state and federal records, documents and forms, including records, documents, and forms stored

electronically on digital devices, that relate to the sale, purchase, transfer or manufacture of firearms, including the Acquisition and Disposition Record, and all receipts of such sales for purposes of determining illegal purchase, transfer or sale of such firearms.

IV. STATEMENT OF PROBABLE CAUSE

A. Recorded Interview of An Ching "Allen" Sun

8. On July 13, 2018, I along with ATF Senior Industry Operations Investigator James Palm interviewed An Ching "Allen" Sun ("SUN"), a former EXA Tactical Firearms employee who wished to speak to ATF regarding EXA Tactical Firearms owner LEE.[1] SUN told me that he worked for LEE at EXA Tactical Firearms as a salesperson from October 2016 until January of 2018. SUN said that, as a salesperson, he would complete the initial necessary Dealers Record of Sales ("DROS") paperwork to begin a firearms transaction and logging firearms into and out of the A&D record at the **SUBJECT PREMISES**. SUN said much of LEE'S records of previous sales were often erroneous or misplaced altogether. SUN said this was particularly the case with many of the Private Party Transfers ("PPT") for "unsafe" (i.e., "off-roster") firearms.

a. DROS is an application to purchase or otherwise acquire a firearm in California, and contains transaction

[1] After the interview was concluded, SUN asked me if his employment at and association with EXA Tactical Firearms would negatively impact his application to become a Naturalized U.S. Citizen. SUN is currently a Lawful Permanent Resident (Green Card holder). I told him that it should not have any impact on his application, but no promises of benefits or other consideration were made to SUN.

information, such as firearm description and purchaser identifiers.

b. "Unsafe" handgun means a handgun that is not on the roster of handguns certified for sale in the State of California. Any new handgun sold in the State of California must pass the State of California required safety testing. Handguns that pass this safety testing are put on a roster of firearms legal for sale to the general public in the State of California. Licensed firearms dealers are prohibited from selling "unsafe" (i.e., "off-roster") handguns directly to the general public, but they may be sold to sworn members of a qualified law enforcement agency. Rules governing "unsafe" handguns do not apply when the sale, loan, or transfer is made during a PPT.

c. A PPT is a firearms transaction where neither party to the transaction is a licensed dealer, but the sale, loan, or transfer of the firearm must be completed through a licensed firearms dealer.

d. An A&D record is used by an FFL and is a written acquisition and disposition book used to log all incoming and outgoing firearms, unless the FFL has a computer variance from ATF to store acquisition and disposition material on a computer. Based on my training and experience, these are required to be kept at the **SUBJECT PREMISES**.

9. SUN told me that he recalled many instances where LEE and EXA Tactical Firearms used the PPT "loophole" in order to sell "unsafe" handguns that they took into inventory, even

though these firearms were brand new and in original packaging from the manufacturer. SUN said that on more than one occasion LEE asked him to alter the description of the firearm on the transaction paperwork from an "unsafe" handgun to a California compliant handgun. SUN also told me that LEE illegally used his (SUN's) personal information for a PPT on an "unsafe" firearm that was purposely not correctly logged into the A&D record. SUN also recalled instances where LEE released a firearm to a regular customer before the 10-day waiting period had expired and also that LEE would approve a transaction after the 30-day DROS expiration date. All of these instances occurred at the **SUBJECT PREMISES**. SUN further explained to me that these types of firearms ("unsafe") can bring much more profit because of the demand for these handguns is so high.

B. Recorded Interview of Elizabeth McDowell

10. On July 17, 2018, I, along with SIOI Palm, interviewed Elizabeth McDowell ("MCDOWELL"), a former employee of EXA Tactical Firearms, who also wished to speak to ATF regarding the business practices of owner LEE.[2] MCDOWELL told me that she worked as a salesperson at EXA Tactical Firearms from February to September of 2016, initiating DROS transaction paperwork and making the requisite entries into the A&D book.

[2] United States Secret Service Special Agent Casey Horrigan informed me that MCDOWELL has been indicted in Case No. CR 18-00513 for violating Title 18, United States Code, Section 1028A(a)(1) (Aggravated Identity Theft). That case remains pending as of the date of this affidavit. I have been informed that as of the date of this affidavit no promises of leniency or other benefits have been conveyed to MCDOWELL in exchange for her providing information to the government.

11. MCDOWELL told me that on more than one occasion, LEE would use the personal information of a local police officer who was a friend and regular customer of LEE's to initiate an "unsafe" handgun transaction to another party as a PPT, without that officer being present at the **SUBJECT PREMISES**. MCDOWELL also said that LEE gave that officer access to his personal DROS Entry System account to initiate or assist in firearm transactions at the **SUBJECT PREMISES**. Furthermore, this officer was used as the "Transferor" on PPTs for "unsafe" handguns without being present or necessarily aware of the transaction.

C. Previous Industry Operations Inspection Results and Database Search Results

12. SIOI Palm told me that previous Inspections of EXA Tactical Firearms in 2014 and 2015 revealed numerous violations, including the failure to completely record firearm acquisition and dispositions in the A&D record, as well as the failure to report multiple sales.

13. SIOI Palm also informed me that on June 22, 2016, agents from the California Department of Justice, Bureau of Firearms, seized approximately nineteen assault rifles from EXA Tactical Firearms, which were in violation of state laws pertaining to assault weapons.

14. On October 22, 2018, SIOI Palm assisted me in querying the ATF Federal Licensing System (FLS), and I learned that LEE is listed as the responsible party (licensee) for EXA Tactical Firearms, at 151 South 9th Street, La Puente, California using Manufacturing License number 995037078E01729, Pawn License

number 995037020K02032, and Importer License number 995037080K02034.

15. On November 26, 2018, SIOI Palm showed me the results of his query into the California Department of Justice DROS system, and I learned that from October 2017 to October 2018 EXA Tactical Firearms transferred approximately 85 unsafe firearms that are prohibited for sale to non-law enforcement individuals under California Penal Code Section 2000. In order to accomplish the unlawful transfer, EXA Tactical Firearms violated the California Gun Control Act of 1968 and fraudulently claimed that each transaction fell into one of two exceptions to California Penal Code Section 2000: that the firearm was a Curio or Relic ("C&R") or that the firearm was transferred from a private party, i.e. through a PPT. Based on my knowledge of this investigation, EXA Tactical Firearms and LEE have not initiated any transactions since LEE's DROS account was made inactive in late September/early October 2018.

16. Based on my review and SIOI Palm's review of the DROS records, which is detailed more fully below, I believe EXA Tactical Firearms and LEE are circumventing California Penal Code section 2000 by transferring "unsafe handguns" directly to otherwise prohibited persons in two ways:

a. EXA Tactical Firearms and LEE are transferring "unsafe" firearms directly to otherwise prohibited persons via the PPT exemption from the **SUBJECT PREMISES**.

i. In these PPT transactions, EXA Tactical Firearms and LEE record either LEE or another person's

information as the transferring party, when, in fact, the firearms are being sold directly from EXA Tactical Firearms' inventory. Put differently, rather than record the transfer as a transfer from EXA Tactical Firearms to the buyer, EXA Tactical Firearms and LEE record the transfer as between two private parties. The transaction is falsely structured this way because EXA Tactical Firearms would otherwise be prohibited from transferring the "unsafe" firearm directly to the buyer under California law.

ii. From April 2018 to September 2018, EXA Tactical Firearms transferred approximately 51 handguns falsely claiming the transfer occurred as a PPT: April 2018 – 1 PPT sale; May 2018 – 2 PPT sales; June 2018 – 10 PPT sales; July 2018 – 16 PPT sales; August 2018 – 18 PPT sales; September 2018 – 4 PPT sales.

iii. A review of DROS records indicates that all 51 of these transactions occurred without an initial purchaser, which violates 18 U.S.C. §§ 922(t)(1) and 922(b)(5). An initial purchase should occur between a dealer-transferor (FFL) to a private party. A PPT should only occur after an initial transfer from an FFL to a private party in an initial purchase. ATF records indicate that the 51 firearms discussed above were transferred to EXA Tactical Firearms and the next transaction recorded was a PPT. There was no intervening initial purchase for these firearms from EXA Tactical Firearms (a FFL) to a private party. Falsifying records also violates 27 C.F.R. § 478.124.

iv. From October 2017 to October 2018, 20 of these PPT transactions listed LEE as the initial transferor of the firearms. Based on my training and experience, I know that generally all handguns imported into the State of California must be imported by a FFL. Because there is no record of an initial transfer from EXA Tactical Firearms to LEE for these 20 firearms, I believe the firearms were transferred from EXA Tactical Firearms to LEE without executing an ATF Form 4473, in violation of 18 U.S.C. § 922(a)(6). An ATF Form 4473 must be filled out and recorded every time there is a transfer of a firearm from an FFL to a private party. Because EXA Tactical Firearms is the FFL, not LEE, then the transfer from EXA Tactical Firearms to LEE is a transfer from an FFL to a private party and an ATF Form 4473 was required to be filled out and recorded. Based on my review of the California DROS database, none of these 20 firearm transfers were recorded as initial purchases by LEE from EXA Tactical Firearms. Therefore, based on my training and experience, and discussions with SIOI Palm, I believe that neither EXA Tactical Firearms nor LEE filled out and recorded an ATF Form 4473 for the 20 firearms transferred from EXA Tactical Firearms to LEE between October 2017 and October 2018. LEE subsequently transferred these 20 firearms from the **SUBJECT PREMISES** to other private parties and recorded the transfers as PPTs, in violation of 18 U.S.C. §§ 922(a)(1)(A), 922(b)(2), and 27 C.F.R. § 478.125(e).

b. EXA Tactical is also transferring "unsafe" firearms via the Curio or Relic transfer exemption in the

California DROS system.

i. Under California law there is an exemption from the general prohibition on the sale of "unsafe" firearms to the general public, if the firearm being transferred is over 50 years of age or is a firearm listed in ATF Publication 5300.11 Curios or Relics List. Based upon my review and SIOI Palm's review of the DROS database, I believe EXA Tactical Firearms and LEE are transferring new "unsafe" firearms from the **SUBJECT PREMISES** to the general public by logging the sale of these new firearms as "Curios or Relics" in the California DROS system. EXA Tactical Firearms and LEE are able to conduct these transfers without detection by the State of California because the California DROS system is unable to cross-reference the make and model of the firearm being transferred with the listed firearms on ATF Publication 5300.11 Curios or Relics List.

ii. To be recognized as C&R per 27 C.F.R. § 478.11 the firearm must fall within one of the three categories:

(I) Firearms which were manufactured at least 50 years prior to the current date, but not including replicas of such firearms;

(II) Firearms which are certified by the curator of a municipal, State, or Federal museum which exhibits firearms to be curios or relics of museum interest; and

(III) Any other firearms which derive a substantial part of their monetary value from the fact that they are novel, rare, bizarre, or because of their association with some historical figure, period, or event.

iii. From October 2017 to October 2018, EXA Tactical Firearms transferred approximately 45 modern handguns (handguns that I and SIOI Palm could identify as being manufactured within the last 50 years based on the make and model of the firearm) to non-law enforcement personnel (i.e. otherwise prohibited persons) by claiming these firearms were C&R. From April 2018 to September 2018, twenty-eight (28) of these transfers of modern handguns as C&R's occurred: April 2018 – 1 C&R sale; May 2018 – 6 C&R sales; June 2018 – 6 C&R sales; July 2018 – 5 C&R sales; August 2018 – 8 C&R sales; and September 2018 – 2 C&R sales.

iv. Based upon my review of the make and model of the handguns and a review of ATF Publication 5300.11, none of the 45 firearms EXA Tactical Firearms reported as C&R firearms in the California DROS System meet the definition of a C&R. By falsifying the information in the DROS system, EXA Tactical Firearms violated 18 U.S.C. § 922(b)(2) and a transfer of a firearm in violation of California Penal Code Section 2000 occurred.

D. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

17. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony

PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise,

scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not

actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents,

programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For

example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed.

A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

h. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

V. CONCLUSION

18. For all the reasons described above, there is probable cause to believe that LEE has committed a violation of Title 18, United States Code, Section 922(m) (Licensed Dealer Knowingly Making Any False Entry In A Required Record); Section 922(b)(2) (Licensed Dealer To Sell Or Deliver Any Prohibited Firearm To A Person In Violation Of State Law); Section 924(a)(3)(A) (Licensed Dealer Makes Any False Statement Or Representation Kept In Required Records); Section 923(g)(1)(A) (Licensed Dealer

//

//

Failure To Maintain Records); and Section 922(a)(1)(A) (Dealing Firearms Without A License).

Ludger A. Parent
Special Agent, ATF

Subscribed to and sworn before me
this day of December 2018.

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

SUBJECT PREMISES TO BE SEARCHED

1. The premises to be searched is described as follows:

a. The premises known as 151 South 9th Street, Unit F, La Puente, California, including all rooms, attics, storage rooms, garages or all outbuildings of any kind, attached or unattached, including all safes located on the premises. Unit F is located on the top floor of a tan stucco two story structure. The front door faces west at the north end of the structure and the letter “F” appears on the door.

ATTACHMENT B

ITEMS TO BE SEIZED:

1. The items to be seized from the **SUBJECT PREMISES** are described as follows:

a. Any and all state and federal records, documents and forms, including records, documents, and forms stored electronically on digital devices, that relate to the sale, purchase, transfer or manufacture of firearms, including the Acquisition and Disposition Record, and all receipts of such sales for purposes of determining illegal purchase, transfer or sale of such firearms.

b. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

c. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software,

as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing

data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not

apply to any search of digital devices pursuant to any other court order.